CFA 00018
US

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００２年１１月１５日

出 願 番 号
Application Number: 特願２００２－３３２５７７

[ST. 10/C]: [ＪＰ２００２－３３２５７７]

出 願 人
Applicant(s): キヤノン株式会社

２００３年１２月 ２日

特許庁長官
Commissioner,
Japan Patent Office 今井康

出証番号 出証特２００３－３０９９３７３

【書類名】　特許願
【整理番号】　226643
【提出日】　平成14年11月15日
【あて先】　特許庁長官殿
【国際特許分類】　H04N　5/00
【発明の名称】　情報処理装置
【請求項の数】　1
【発明者】
【住所又は居所】　東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内
【氏名】　岩村　恵市
【特許出願人】
【識別番号】　000001007
【氏名又は名称】　キヤノン株式会社
【代理人】
【識別番号】　100090273
【弁理士】
【氏名又は名称】　國分　孝悦
【電話番号】　03-3590-8901
【手数料の表示】
【予納台帳番号】　035493
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9705348
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報処理装置

【特許請求の範囲】

【請求項１】　所定の作者により作成された原データを処理する情報処理装置であって、

上記原データを変更する際に、その変更に関する変更情報を記憶媒体に記憶する変更情報記憶手段と、

上記変更情報が原本であることを保証するための変更保証情報を作成する変更保証情報作成手段とを有することを特徴とする情報処理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報処理装置に関し、特に、データの原本性を保証するために用いて好適なものである。

【０００２】

【従来の技術】

近年、コンピュータやインターネットの普及に伴い、情報をデジタル化し、デジタルデータとして利用する形態が一般化しつつある。一方、デジタルデータでは、まったく同質なコピーを容易に生成でき、編集処理も容易に実行できるという特徴がある。そのため、デジタルデータの原本性を保証することは重要である。

【０００３】

一般に、デジタルデータの原本性を保証するには、米国特許第５４９９２９４号明細書（特許文献１）に示されるように、デジタル画像のハッシュ値に公開鍵暗号を用いた電子署名を作成することによって実現できることが知られている。

【０００４】

[米国特許第５４９９２９４号明細書の説明]

上記米国特許第５４９９２９４号明細書（特許文献１）に記載されている技術では、電子署名データを生成するために、ハッシュ関数と公開鍵暗号とを使用し

ている。

【０００５】

上記電子署名とは、送信者がデータと一緒に該データに対応する署名データを送り、受信者がその署名データを検証して該データの正当性を確認することができるようにするものである。

【０００６】

ハッシュ関数と公開鍵暗号とを用いて電子署名データを生成してデータの正当性を確認する方法は、具体的に以下のようになり、これが上記特許文献１に記載されている方法である。

【０００７】

まず、秘密鍵をＫｓ、公開鍵をＫｐとすると、発信者は、平文データＭをハッシュ関数により圧縮して一定長の出力ｈを算出する演算を行う。

【０００８】

次に、秘密鍵Ｋｓで一定長の出力ｈを変換して電子署名データｓを作成する演算を以下の（１式）により行う。

Ｄ(Ks, h)＝ｓ・・・（１式）

その後、該電子署名データｓと平文データＭとを送信する。

【０００９】

一方、受信者は、受信した電子署名データｓを公開鍵Ｋｐで変換する演算を以下の（２式）により行う。

Ｅ(Kp, s)＝Ｅ(Kp, Ｄ(Ks, h''))＝h''　・・・（２式）

【００１０】

また、受信者は、受信した平文データM'を発信者と同じハッシュ関数により圧縮して一定長の出力ｈ'を算出する演算を行う。そして、この演算で算出された一定長の出力ｈ'と、上記（２式）により得られた一定長の出力ｈ''とが一致すれば、受信した平文データM'が正当であると判断する。

【００１１】

平文データＭが送受信間で改ざんされた場合には、上記（２式）により得られた一定長の出力ｈ''と、受信した平文データM'を発信者と同じハッシュ関数に

より圧縮して得られた一定長の出力ｈ’とが一致しないので改ざんを検出できる。

【００１２】

ここで、平文データＭの改ざんに合わせて電子署名データｓの改ざんも行われてしまうと改ざんを検出することができなくなる。しかし、電子署名データｓを改ざんするには、一定値の出力ｈから平文データＭを求める必要があり、このような計算はハッシュ関数の一方向性により不可能である。

【００１３】

次に、ハッシュ関数について説明する。

ハッシュ関数は、上記電子署名データｓの生成を高速化するため等に用いられる。ハッシュ関数は、任意の長さの平文データＭを処理して、一定の長さの出力（一定値の出力）ｈを出す機能を持つ。ここで、一定値の出力ｈを平文データＭのハッシュ値（またはメッセージダイジェスト、デジタル指紋）という。

【００１４】

ハッシュ関数に要求される性質として、一方向性と衝突耐性がある。

上記一方向性とは、一定値の出力ｈを与えた時に、ｈ＝Ｈ（Ｍ）となる平文データＭの算出が計算量的に困難であることである。

上記衝突耐性とは、平文データＭを与えた時に、Ｈ（Ｍ）＝Ｈ（Ｍ’）となる平文データＭ’（Ｍ≠Ｍ’）を算出することが計算量的に困難であること、及びＨ（Ｍ）＝Ｈ（Ｍ’）かつＭ≠Ｍ’となる平文データＭ，Ｍ’を算出することが計算量的に困難であることである。

【００１５】

ハッシュ関数としては、MD-2、MD-4、MD-5、SHA-1、RIPEMD-128、及びRIPEMD-160等が知られており、これらのアルゴリズムは、一般に公開されている。

【００１６】

続いて公開鍵暗号について説明する。

公開鍵暗号は、暗号鍵と復号鍵が異なり、暗号鍵を公開し、復号鍵を秘密に保持する暗号方式である。公開鍵暗号の主な特徴として、以下の３つのことが挙げられる。

（ａ）暗号鍵と復号鍵とが異なり暗号鍵を公開できるため、暗号鍵を秘密に配送する必要がなく、鍵配送が容易である。

（ｂ）各利用者の暗号鍵は公開されているので、利用者は各自の復号鍵のみを秘密に記憶しておけばよい。

（ｃ）送られてきた通信文の送信者が偽者でないこと、及びその通信文が改ざんされていないことを受信者が確認するための認証機能を実現できる。

【００１７】

例えば、平文データＭに対して、公開の暗号鍵Ｋｐを用いた暗号化操作をＥ(Kp, M)とし、秘密の復号鍵Ｋｓを用いた復号化操作をＤ(Ks, M)とすると、公開鍵暗号アルゴリズムは、次の２つの条件を満たす。

【００１８】

（１）公開の暗号鍵Ｋｐが与えられたとき、暗号化操作Ｅ(Kp, M)の計算は容易である。秘密の復号鍵Ｋｓが与えられたとき、復号化操作Ｄ(Ks, M)の計算は容易である。

（２）もし、秘密の復号鍵Ｋｓを知らないのなら、公開の暗号鍵Ｋｐと、暗号化操作Ｅの計算手順と、Ｃ＝Ｅ(Kp, M)を知っていても、平文データＭを決定することは計算量の点で困難である。

【００１９】

次に、上記（１）、（２）の条件に加えて、次の（３）の条件が成立することにより、秘密通信を実現できる。

（３）全ての平文データＭに対し、暗号化操作Ｅ(Kp, M)を定義でき、以下の（４式）が成立する。

Ｄ(Ks, Ｅ(Kp, M))＝Ｍ・・・（４式）

【００２０】

つまり、公開の暗号鍵Ｋｐは公開されているため、誰もが暗号化操作Ｅ(Kp, M)を計算することができるが、復号化操作Ｄ(Ks, Ｅ(Kp, M))を計算して平文データＭを得ることができるのは秘密の復号鍵Ｋｓを持っている本人だけである。

【００２１】

一方、上記（１）、（２）の条件に加えて、次の（４）の条件が成立すること

により認証通信を実現できる。

（４）すべての平文データＭに対し、復号化操作Ｄ(Ks, M)を定義でき、以下の（５式）が成立する。

Ｅ(Kp, Ｄ(Ks, M))＝Ｍ・・・（５式）

【００２２】

つまり、復号化操作Ｄ(Ks, M)を計算できるのは、秘密の復号鍵Ｋｓを持っている本人のみであり、他の人が偽の秘密の復号鍵Ｋｓ'を用いて復号化操作Ｄ(Ks', M)を計算し、秘密の復号鍵Ｋｓを持っている本人になりすましたとしても、上記（５式）が成立しないので（Ｅ(Kp, Ｄ(Ks', M))≠Ｍ）、受信者は、受けとった情報が不正なものであることを確認できる。

【００２３】

また、復号化操作Ｄ(Ks, M)が改ざんされても上記（５式）が成立しなくなり（Ｅ(Kp, Ｄ(Ks, M)')≠Ｍ）、受信者は、受けとった情報が不正なものであることを確認できる。

【００２４】

上記の秘密通信と認証通信とを行うことができる代表例として、RSA暗号やＲ暗号やW暗号等が知られている。

ここで、現在最も使用されている上記RSA暗号による暗号化と復号は、以下の（６式）で示される。

【００２５】

暗号化：暗号化鍵（e, n）　暗号化変換$C=M^e \pmod n$

復号：復号鍵（d, n）　復号変換$M=C^d \pmod n$

$n=p \cdot q$

ここで、p、qは、大きな異なる素数・・・（６式）

【００２６】

【特許文献１】

米国特許第５４９９２９４号明細書

【００２７】

【発明が解決しようとする課題】

しかしながら、米国特許第５４９９２９４号明細書に記載されている手法では、電子署名をつけたデジタルデータを１ビットでも変更した場合、著者が認めた正当な変更であっても、改ざんとして検出される。

【００２８】

さらに、米国特許第５４９９２９４号明細書に記載されている手法では、データを変更した後に関しては、その変更したデータが原本でないことだけが分かるだけである。

【００２９】

例えば、米国特許第５４９９２９４号明細書をデジタルカメラに適用した例を考える。通常、デジタルカメラからの出力であるデジタル画像と電子署名データは、コンピュータ（PC）に取り込まれる。

【００３０】

その後、画像が見やすいように輝度を変更したり、フィルタリングをしたり、または画像を小さくするために余計な部分を切り取ったりすることは通常よく行われる。

【００３１】

これらの処理は、画像を見やすく、分かりやすくするための処理であり、デジタル画像の著作者が認めている処理である場合が多い。しかしながら、米国特許第５４９９２９４号明細書に記載されている技術では、デジタルカメラから出力された後に行われた全ての処理は改ざんとして検出される。

【００３２】

このように従来の技術では、電子署名などによりデータの原本性が保証されているような場合には、上記データを正当なデータとして変更することができないという問題点があった。

【００３３】

本発明は上述の問題点に鑑みてなされたものであり、データの原本性を保証しながら、上記データの作者が認める正当な変更を行えるようにすることを目的とする。

【００３４】

【課題を解決するための手段】

本発明の情報処理装置は、所定の作者により作成された原データを処理する情報処理装置であって、上記原データを変更する際に、その変更に関する変更情報を記憶媒体に記憶する変更情報記憶手段と、上記変更情報が原本であることを保証するための変更保証情報を作成する変更保証情報作成手段とを有することを特徴としている。

【００３５】

【発明の実施の形態】

（第１の実施の形態）

次に、本発明の情報処理装置の第１の実施の形態を、図面を参照しながら説明する。なお、ここではオリジナルのデジタルデータを原画像と呼ぶが、本実施の形態で適用されるデジタルデータ（原データ）は、デジタル画像だけに限らず、デジタルデータ全てに適用できる。

【００３６】

まず、原画像に対する電子署名を生成する。これは、前述した米国特許第５４９９２９４号明細書のように、原画像に対するハッシュ値を生成し、それに対して秘密鍵で電子署名を作成することによって実現できる。この電子署名を第１の署名（図１の署名０）１１と表し、図１（ａ）に示されるように原画像１２とともに保存する。

【００３７】

次に、保存された原画像１２に対して第１の処理を施して、その処理結果を正当な画像として認める場合を考える。上述した米国特許第５４９９２９４号明細書に記載されている電子署名の原理は、デジタルデータ全てに使える公知の技術である。したがって、上述した米国特許第５４９９２９４号明細書に記載されている電子署名の原理を用いて、履歴情報１３に対する電子署名を作成する。ここで、履歴情報１３とは、上記第１の処理で行われた原画像１２の変更（履歴）に関する情報である。なお、以下の説明では、この履歴情報１３に対する電子署名を第２の署名（図１の署名１）１４と称する。

【００３８】

例えば、上記第１の処理が、フォトッショップver.Xというエディタで行った輝度変換である場合、上記第１の処理に対する履歴情報１３は、対象画像を特定する情報と、エディタを特定する情報と、上記エディタで規定されている輝度変換というフィルタ名と、それに用いたパラメータ情報などから構成される。

【００３９】

また、履歴情報１３は、原画像１２と変更画像との差分データを含んでいても良い。ここで、対象画像を特定する情報は、原画像１２のID番号や、原画像１２の署名である第１の署名（図１の署名０）などを用いることができる。ただし、履歴情報１３が長い場合には、ハッシュ値を生成し、それに署名してもよい。そして、このようにして作成された履歴情報１３と第２の署名１４を図１（ｂ）に示されるように原画像１２と一緒に保存する。

【００４０】

上記の処理は、著作者によって行われる処理である。次に、上記第１の処理により輝度変換された画像の入手を他のユーザが希望している場合を考える。著作者は、図１（ｂ）のように、記憶媒体に保存されている原画像１２、第１の署名（図１の署名０）１１、履歴情報１３、及び第２の署名（図１の署名１）１４を、通信手段を用いてそのユーザに送信する。以下、これらの情報が送られたユーザが行う検証処理について説明する。

【００４１】

まず、原画像１２に対する第１の署名（図１の署名０）１１を確認する。この処理は、前記の米国特許第５４９９２９４号明細書において説明した検証処理と同じ手法によって実現できる。次に、履歴情報１３に対する第２の署名（図１の署名１）を確認する。これも電子署名の確認手順（上記検証処理）により実現できる。

【００４２】

この２つのデータの正当性が電子署名により確認された後、履歴情報１３に書かれた上記第１の処理と同じ処理を、原画像１２に対して行うことにより、ユーザは、輝度変換された画像を得ることができる。

【００４３】

図４は、以上のような処理を行う本実施形態の情報処理装置の構成の一例を示したブロック図である。なお、本発明の情報処理装置の実現に当たっては、図３に示される全ての機能を使用することは必須ではない。

【００４４】

図４において、情報処理装置（コンピュータ）３０１のハードウェアは、一般に普及しているパーソナルコンピュータであり、スキャナ等の画像入力装置３１７から読み取られた画像を入力し、編集や保管を行うことが可能である。

【００４５】

また、画像入力装置３１７で得られた画像をプリンタ３１６から印刷させることができる。なお、ユーザからの各種指示等は、マウス３１３やキーボード３１４などからの入力操作により行われる。

【００４６】

コンピュータ３０１の内部では、バス３０７により後述する各ブロックが接続され、種々のデータの受け渡しが可能である。図３において、ＭＰＵ３０２は、コンピュータ３０１内部の各ブロックの動作を制御し、あるいは内部に記憶されたプログラムを実行することができる。

【００４７】

主記憶装置３０３は、ＭＰＵ３０２において行われる処理のために、一時的にプログラムや処理対象の画像データを格納しておく装置である。ハードディスク（ＨＤＤ）３０４は、主記憶装置３０３等に転送されるプログラムや画像データをあらかじめ格納したり、処理後の画像データを保存したりすることのできる装置である。

【００４８】

スキャナインタフェース（Ｉ／Ｆ）３１５は、原稿やフィルム等を読み取って、画像データを生成するスキャナ３１７と接続され、スキャナ３１７で得られた画像データを入力することのできるインターフェース（Ｉ／Ｆ）である。

【００４９】

プリンタインタフェース３０８は、画像データを印刷するプリンタ３１６と接続され、印刷する画像データをプリンタ３１６に送信することのできるインター

フェース（Ｉ／Ｆ）である。

【００５０】

ＣＤドライブ（ＣＤ）３０９は、外部記憶媒体の一つであるＣＤ（ＣＤ－Ｒ／ＣＤ－ＲＷ）に記憶されたデータを読み出したり、あるいは書き込んだりすることができる装置である。

【００５１】

ＦＤＤドライブ（ＦＤＤ）３１１は、ＣＤドライブ３０９と同様に、外部記憶装置の一つであるＦＤＤからの読み出しや、ＦＤＤへの書き込みをすることができる装置である。

【００５２】

ＤＶＤドライブ（ＤＶＤ）３１０は、ＦＤＤドライブ３１１と同様に、外部記憶装置の一つであるＤＶＤからの読み出しや、ＤＶＤへの書き込みをすることができる装置である。

【００５３】

なお、ＣＤ、ＦＤＤ、ＤＶＤ等に画像編集用のプログラム、あるいはプリンタドライバが記憶されている場合には、これらプログラムをハードディスク（ＨＤＤ）３０４上にインストールし、必要に応じて主記憶装置３０３に転送されるようになっている。

【００５４】

インターフェース（Ｉ／Ｆ）３１２は、マウス３１３やキーボード３１４からの入力指示を受け付けるために、これらと接続されるインターフェース（Ｉ／Ｆ）である。

【００５５】

また、モニタ３０６は、透かし情報の抽出処理結果や処理過程を表示することのできる表示装置である。さらに、ビデオコントローラ３０５は、表示データをモニタ３０６に送信するための装置である。

【００５６】

なお、本実施の形態では、情報処理装置３０１に上述した機能を全て搭載するようにしたが、上述した機能を分配して複数の装置からなるシステムとしてもよ

い。すなわち、複数の機器（例えば、ホストコンピュータ、インターフェース機器、リーダ、プリンタ等）から構成されるシステムにしても、一つの機器からなる装置（例えば、複写機、ファクシミリ装置等）にしてもよい。

【００５７】

次に、図２と図３を参照しながら、本実施の形態の情報処理装置３０１の動作について説明する。図２は、電子署名を生成する際の情報処理装置３０１の処理を説明するフローチャートである。また、図３は、電子署名を検証する際の情報処理装置３０１の処理を説明するフローチャートである。

【００５８】

なお、原画像１２に対する第１の署名（図１の署名０）を生成する際の処理は、上述した米国特許第５４９９２９４号明細書に記載されている技術と同様にして行えるので説明を省略し、ここでは、原画像１２と第１の署名（図１の署名０）１１が、情報処理装置３０１内の記憶媒体に保存されているという前提で説明する。

【００５９】

まず、図２に示す電子署名（第２の署名（図１の署名１）１４）を生成する際の処理を説明する。なお、以下では必要に応じてこの処理を署名生成処理と称する。

記憶媒体に保存された原画像１２を入力する（ステップＳ２０１）。これは、ハードディスク（ＨＤＤ）３０４、ＣＤドライブ（ＣＤ）３０９、ＤＶＤドライブ（ＤＶＤ）３１０、またはＦＤＤドライブ（ＦＤＤ）３１１などに接続された各記憶媒体に格納されている原画像１２を、マウス３１３やキーボード３１４からの入力指示により、主記憶装置３０３にロードすることにより実現される。

【００６０】

次に、その原画像１２に対して変更処理を行う（ステップＳ２０２）。このときに行った変更処理に関する履歴情報１３（上記記対象画像特定情報や、エディタ特定情報、処理を特定するフィルタリング名やそのパラメータなど）を記憶媒体に記憶する（ステップＳ２０３）。

【００６１】

なお、この変更処理は、複数の処理を組み合わせても良い。また、変更処理を行った結果、変更処理した画像が正当であると認められない場合には、処理結果及び処理履歴を廃棄し、前の画像（原画像１２）に戻すこともできる。

【００６２】

そして、これらの処理は、マウス３１３やキーボード３１４からの入力指示に応じて主記憶装置３０３にロードしたプログラムを、ＭＰＵ３０２などを用いて実行することにより行われる。このとき、モニタ３０６により実行状況や、その結果をモニタすることも可能である。

【００６３】

次に、その処理結果を正当な画像として認める場合（ステップＳ２０４）、記憶媒体に記憶された履歴情報１３に対して電子署名（第２の署名（図１の署名１）１４）を作成する（ステップＳ２０５）。これらの処理も、マウス３１３やキーボード３１４からの入力指示に応じて主記憶装置３０３にロードしたプログラムを、ＭＰＵ３０２などを用いて実行することにより行われる。

【００６４】

最後に、生成した原画像１２、第１の署名（図１の署名０）１１、履歴情報１３、及び第２の署名（図１の署名１）１４を、ハードディスク３０４、ＣＤドライブ３０９、ＤＶＤドライブ３１０、またはＦＤＤドライブ３１１などに保存する（ステップＳ２０６）。

【００６５】

次に、図３に示す電子署名を検証する際の処理を説明する。なお、以下では、必要に応じてこの処理を署名検証処理と称する。

なお、電子署名（第１の署名１１及び第２の署名１４）の検証処理を行うときには、第１の署名（図１の署名０）１１、履歴情報１３、及び第２の署名（図１の署名１）１４を、情報処理装置３０１が持っていることを前提とする。ただし、以下の処理も、図４に示す情報処理装置３０１、特に、マウス３１３やキーボード３１４からの入力指示により主記憶装置３０３にロードしたプログラムを、ＭＰＵ３０２などを用いて実行することにより行われる。

【００６６】

まず、原画像１２に対する第１の署名（図１の署名０）１１を確認する（ステップＳ２１１）。次に、履歴情報１３に対する第２の署名（図１の署名１）１４を確認する（ステップＳ２１２）。

【００６７】

次に、この２つのデータ（原画像１２と履歴情報１３）の正当性が、電子署名（第１の署名１１と第２の署名１４）により確認された場合には（ステップＳ２１３）、履歴情報１３に書かれている処理と同じ処理を原画像１２に対して行う。これにより、ユーザは、輝度変換された画像を得る（ステップＳ２１４）。

【００６８】

一方、ステップＳ２１３において、署名が正しくないと判定された場合には、原画像１２及び履歴情報１３のうちの少なくとも何れか一方は正しくないので処理を中止する。また、このように署名が正しくない場合には、情報（原画像１２、履歴情報１３）に改ざんがあることをユーザに通知するようにしてもよい。

【００６９】

以上のように、本実施の形態では、原画像１２に対する第１の署名（図１の署名０）１１を保持するようにしたので、原画像１２に対する原本性を保証できる。

そして、履歴情報１３に対する第２の署名（図１の署名１）１４を保持するようにしたので、原画像１２の変更処理に対する正当性を保証できる。したがって、原画像１２に対して、著作者が認める正当な変更を行うことができ、画像の最新性を保証できる。

【００７０】

ところで、上述したように、米国特許第５４９９２９４号明細書に記載されている技術では、例えば、デジタルカメラから出力された後に行われた全ての処理は改ざんとして検出される。

【００７１】

そこで、著者が自分の署名用の秘密鍵を用いて、変更を認めた変更画像に対して電子署名をつけるという解決策が考えられる。しかしながら、この場合、署名した変更画像は独立した画像となり、原画像１２と、原画像１２を変更すること

により得られる変更画像との関係が分からなくなるという問題点が残る。さらに、いくつかの変更を著者が正当と認めた場合、多くの画像と署名のペアを管理する必要があり、メモリ的な制約もでてくる可能性がある。

【００７２】

これに対して本実施の形態では、第１の署名（図１の署名０）１１及び第２の署名（図１の第２の署名１）１４が正しければ、原画像１２と変更画像との間の関係（処理履歴）を履歴情報１３により知ることができる。

【００７３】

さらに、履歴情報１３は、変更画像に比べてデータ量が少ないので、多くの履歴情報１３を保存しても、それに対応する変更画像をすべて保存することに比べてメモリ容量が小さくなる。これは、後述する第２の実施の形態に示す複数回の変更処理に対して特に有効である。

【００７４】

また、履歴情報１３と署名情報（第１の署名１１、第２の署名１４）は、画像情報に比べて小さいので、原画像１２のヘッダなどに格納することが容易で、多くの履歴情報１３があっても１つのファイルとして管理できる。これも後述する第２の実施の形態に示す複数回の変更処理に対して特に有効である。

【００７５】

（第２の実施の形態）

次に、本発明の第２の実施の形態を説明する。なお、本実施の形態の説明において、上述した第１の実施の形態と同一の部分については同一の符号を付して詳細な説明を省略する。

【００７６】

上述した第１の実施の形態では、１回の処理に対する例を示したが、本実施の形態では、第１の処理の後に、第２の処理、第３の処理・・・と続けてそれらを正当な処理として認められるようにしている。すなわち、本実施の形態では、以下に示すようにして、原画像１２の原本性を保証しながら、複数回の変更処理による画像の最新性を保証できるようにしている。

【００７７】

例えば、第１の実施の形態の情報処理装置３０１で生成した履歴情報１３を第１の履歴（図５の履歴１）と表す。第１の実施の形態では、図２のフローチャートに従って行われる処理の前提として、原画像１２と第１の署名（署名０）１１は保存されているとしたが、本実施の形態では、２回目の変更に対しては第１の履歴（図５の履歴１）１３と、それに対する第２の署名（署名１）１４も保存されているとして、図２のフローチャートに従った処理を行う。

【００７８】

その結果、２回目の変更に対する履歴情報として第２の履歴（図５の履歴２）１５と、この第２の履歴１５に対する電子署名である第３の署名（図５の署名２）１６とが生成される。その結果、原画像１２、第１の署名（署名０）１１、第１の履歴（履歴１）１３、及び第２の署名（署名１）１４に加えて、第３の履歴（図５の履歴２）１５と第２の署名（図５の署名２）１６とが保存される。

【００７９】

以下同様にして変更処理を繰り返せば、Ｎ（Ｎは自然数）回の変更処理に対して、原画像１２と、第１～第Ｎの履歴（図５の履歴１～履歴Ｎ）と、第１～第（Ｎ＋１）の署名（図５の署名０～署名Ｎ）とが署名生成処理によって生成され、保存されることになる（図５（ａ）を参照）。

【００８０】

一方、この署名生成処理に対する署名検証処理では、図３のフローチャートにおけるステップＳ２１１の処理、すなわち原画像１２に対する署名確認の処理を行った後に、ステップＳ２１２において、第２の署名（署名１）１３の検証だけでなく、第３～第Ｎ＋１の署名（図５の署名２～署名Ｎ）（についても検証を行う。そして、ステップＳ２１３において、これら第２～第（Ｎ＋１）の署名（図５の署名１～署名Ｎ）が正しいと判断された場合には、ステップＳ２１４において、原画像１２に対し、第１～第Ｎの履歴（図５の履歴１～履歴Ｎ）の処理を実行し、原画像１２を変更する。

【００８１】

なお、この場合において、第２～第Ｍ（Ｍは、（Ｎ＋１）より小さい自然数）の署名までは正しく、それ以降の署名が正しくない場合には、全ての処理を中止

しなくても第２～第Ｍの署名に対する処理を行い、それ以降の署名に対する処理を中止することもできる。

【００８２】

以上のように本実施の形態では、１～Ｎ回目の変更に対する履歴情報である第１～第Ｎの履歴と、この第１～第Ｎの履歴に対する電子署名である第２～第（Ｎ＋１）の署名とを生成するようにし、第１～第Ｎの履歴が正しいかどうかを、第２～第（Ｎ＋１）の署名を用いて判断し、正しい場合には第１～第Ｎの履歴に従って原画像１２を変更するようにしたので、１回の変更だけでなく、著作者が正当と認めれば複数回の変更処理を追加しても画像の最新性を常に保証できる。

【００８３】

なお、著作者が、第１の処理を含まない新たな第２の処理も正当と認める場合には、第１の処理の代わりに第２の処理の履歴情報に対して図２と図３に示したフローチャートに従った処理を行えば、第２の処理に対する変更の正当性と原本性とが第１の実施の形態と同様にして保証できることは明らかである。この場合、第１の処理と第２の処理に関する関係は、図５（ｂ）のようになる。このとき、図６に示すようなリスト６０に、履歴情報と電子署名とを処理ごとにまとめて別管理したり、履歴情報のなかにその処理の目的・効果などのアブストラクト的な情報を入れておいたりすることもできる。

【００８４】

（第３の実施の形態）

次に、本発明の第３の実施の形態を説明する。なお、本実施の形態の説明において、上述した第１及び第２の実施の形態と同一の部分については同一の符号を付して詳細な説明を省略する。

【００８５】

上述した第１及び第２の実施の形態では、処理の変更はすべて著作者が行う例を示したが、本実施の形態では、多くのユーザが１つのデジタルデータを変更することができるようにする。ここでは、デジタルデータとして電子文書を想定する。

【００８６】

そして、図７に示すように、複数のユーザ６０３～６０５がサーバ６０１上で共有している電子文書６０２を、ネットワーク６００を介して各ユーザ６０３～６０５が取り込んで完成させる場合を想定する。

【００８７】

なお、上記においてユーザ６０３～６０５とは、ユーザが所有する端末のことであり、この端末のハードウェアは、例えば図４に示した情報処理装置３０１により構成されるものである。以下、サーバ６０１及びユーザ６０３～６０５における処理の内容について説明する。

【００８８】

まず、ユーザ６０３が最初のたたき台となる電子文書６０２を作成し、作成した電子文書６０２を第１の文書として、それに対する署名をつけてサーバ６０１に保存する。なお、以下の説明では、第１の文書に対する署名を第１の署名と称する。また、この第１の署名は、上述した第１及び第２の実施の形態で説明した第１の署名（署名０）１１と同じ方法で作成される。

【００８９】

次に、サーバ６０１に保存された電子文書６０２をユーザ６０４が修正したい場合、ユーザ６０４は、まず、第１の文書とそれに対する第１の署名を確認する。それが正当であれば、第１の文書に対して修正を施して第２の文書を作成し、その修正に関する履歴情報と、この履歴情報に対する署名を付加して保存する。

【００９０】

なお、以下の説明では、この第１の文書の修正に関する履歴情報を第１の履歴情報と称する。また、第１の履歴情報に対する署名を第２の署名と称する。そして、これら第１の履歴情報と第２の署名は、それぞれ上述した第１及び第２の実施の形態で説明した第１の履歴情報（履歴１）１３と第２の署名（署名１）１４と同じ方法で作成される。

【００９１】

次に、ユーザ６０５が修正したい場合、ユーザ６０５は、それまでの署名（第１の署名と第２の署名）を確認し、それらが正当であれば、第２の文書の修正を施して第３の文書を生成し、その修正に関する履歴情報と、この履歴情報に対す

る署名を付加して保存する。

【００９２】

なお、以下の説明では、第２の文書の修正に関する履歴情報を第２の履歴情報と称する。また、第２の履歴情報に対する署名を第３の署名と称する。また、これら第２の履歴情報と第３の署名は、それぞれ上述した第１及び第２の実施の形態で説明した第２の履歴情報（履歴２）１５と第３の署名（署名２）１６と同じ方法で作成される。

【００９３】

以下、他のユーザまたは同じユーザが文書の修正を繰り返したい場合、修正に関する履歴情報と、この履歴情報に対する署名を付加していくことにより、複数のユーザによる電子文書の管理を実現することができる。

【００９４】

ただし、あるユーザが、それまでの署名を確認したときに、署名が正当でなければその旨を他のユーザに通知する。また、あるユーザが、第１～第Ｍ（Ｍは自然数）の履歴情報までの修正は良いと思うが、それ以降の修正は良くないと思う場合には、良いと思う履歴情報までの修正を行った第Ｍの文書を作成し、そのあと第（Ｍ＋１）の履歴情報とは異なる修正を行う。その後、第Ｍの文書を対象文書として特定する情報（文書番号やハッシュ値など）を履歴情報に入れて、その署名を作成することもできる。この場合、第２の実施の形態で説明した図５（ｂ）のように、作成した署名がそれまでの署名と並列の関係になるので、文書管理システムの中に図６のような署名の関係を示すリスト６０を作成し、分かりやすくすることも可能である。

【００９５】

（第４の実施の形態）

次に、本発明の第４の実施の形態を説明する。なお、本実施の形態の説明において、上述した第１～第３の実施の形態と同一の部分については同一の符号を付して詳細な説明を省略する。

【００９６】

本実施の形態では、医療画像に対する医療画像管理システムを例にとり説明す

る。

システムとしては、図７と同様に、複数のユーザ（医者）６０３～６０５がデジタルレントゲン画像などの電子化された医療画像６０２をネットワーク６００で接続されたサーバ６０１上に共有している場合を想定する。

【００９７】

この場合、医療画像６０２に対する原本性を保証するための情報である第１の署名は、デジタルレントゲン機器に保存されているか、またはデジタルレントゲン機器における医療画像６０２の出力時点で生成され、サーバ６０１に保存されているとする。

【００９８】

まず、医者６０３が医療画像６０２を見る場合、画像内容に関する編集は行わないが輝度変換などの視覚的効果に関する変更を行う。このとき、医者６０３は、毎回その輝度変更を行わないようにするために、原画像である医療画像６０２と変更画像との差分をとり、対象画像を特定する情報や上述したその変更に関するアブストラクト的な情報を、医療画像６０２に付加して第１の履歴情報として保存する。

【００９９】

そして、この第１の履歴情報のハッシュ値に自分の署名を生成し、第２の署名としてサーバ６０１に保存するか、または自分（医者６０３）が所有する端末に保存する。なお、これら第１の履歴情報と第２の署名は、それぞれ上述した第１～第３の実施の形態で説明した第１の履歴情報（履歴１）１３と第２の署名（署名１）１４と同じ方法で作成される。

【０１００】

次に、医者６０４が医療画像６０２を見る場合、その原本性を第１の署名により確認し、他の医者６０３の処理を確認するために第１の履歴情報の正当性を第２の署名により確認し、それを利用またはさらに処理を追加する。

【０１０１】

ここで、処理を追加する場合は、第１の履歴情報に従った変更が施された医療画像を変更対象とする場合には、変更対象とする画像に対する情報として第２の

署名を第２の履歴情報に含め、さらに、変更対象とする画像と、自分が作成した変更画像との差分画像などを加えて、第３の署名を生成する。また、原画像（医療画像６０２）を変更対象とする場合、第１の署名を第２の履歴情報に含め、さらに、原画像（医療画像６０２）と、自分が作成した変更画像との差分画像などを加えて、第３の署名を生成する。

【０１０２】

以下、同様の処理を行うことにより、本実施の形態の医療画像管理システムにおいて、原画像の原本性と変更処理の正当性、及び画像の最新性を同時に実現できる。なお、上記において、第２の履歴情報と第３の署名は、それぞれ上述した第１～第３の実施の形態で説明した第２の履歴情報（履歴２）１５と第３の署名（署名２）１６と同じ方法で作成される。

【０１０３】

（第５の実施の形態）

次に、本発明の第５の実施の形態を説明する。なお、本実施の形態の説明において、上述した第１～第４の実施の形態と同一の部分については同一の符号を付して詳細な説明を省略する。

【０１０４】

本実施の形態では、著作物管理システムを用いたビジネスモデルに関する説明を行う。

ここでは、ネットワークに複数のユーザと原画像に対し１次著作権を保有する著作者がある場合を考える。よって、著作者は、図１（ａ）のように、原画像１２とそれに対する第１の署名（署名０）１１を有しているとする。

【０１０５】

図８のフローチャートを参照しながら、本実施の形態のシステムにおける処理を説明する。

まず、著作者は、課金などにより正当と認められたユーザに対して、原画像１２を配布する（ステップＳ７０１）。ただし、この原画像１２には、電子透かしなどの著作権保護のための仕組みが入っていても良い。また、この原画像１２には、上述した原本性を示す第１の署名（署名０）１１も添付され配布される。配

布された原画像１２については、ユーザの利用範囲内で変更することが認められているが、原画像１２を含むその変更画像の配布は認められていないとする。

【０１０６】

ユーザは、各々、原画像１２の署名を確認した後、著作者から配布された原画像１２に対して、いくつかの変更を試みる（ステップＳ７０２）。ユーザが面白いと思った変更画像を正当な２次著作物としたい場合、ユーザは、著作者に、原画像１２と第１の署名（署名０）１１に加えて自ら行った変更に関する履歴情報である第１の履歴情報１３とその電子署名である第２の署名（署名１）１４を著作者に送る（ステップＳ７０３）。ただし、第２の署名（署名１）１４は、ユーザの秘密鍵で署名されており、それを確認する公開鍵も一緒に送付することができる。

【０１０７】

著作者は、第１の署名（署名０）１１と、第２の署名（署名１）１４を確認し、原画像１２に対して第１の履歴情報１３に応じた処理を施す（ステップＳ７０４）。著作者がその処理結果を判定して（ステップＳ７０５）、２次著作物として許諾する場合には、第１の履歴情報１３に対して著作者の鍵による電子署名を生成し、原画像１２と第１の署名（署名０）１１と、第１の履歴情報１３と、第２の署名（署名１）１４と、第３の署名（署名２）１６とを一緒に保存する（ステップＳ７０６）。一方、許諾しない場合は第３の署名（署名２）１６を生成せずに、その旨をユーザに通知する。

【０１０８】

これにより、著作者は、原画像１２である１次著作物から効率的に２次著作物を生成する仕組みを実現することができ、各ユーザは、自分が生成した２次著作物を正当に認められる仕組みを実現することができる。このとき、著作者は複数の２次著作物からの著作権料を得ることができ、各ユーザは１次著作物を基に容易に２次著作物を生成でき、それによる２次著作権料も得ることができる。さらに、３次著作物以降に対しても全く同様にして適用できる。

【０１０９】

（その他の実施の形態）

本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記録媒体（または記憶媒体）を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはＣＰＵやＭＰＵ）が記録媒体に格納されたプログラムコードを読み出し実行することによっても、達成されることは言うまでもない。この場合、記録媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記録した記録媒体は本発明を構成することになる。

【０１１０】

また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているオペレーティングシステム（ＯＳ）などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【０１１１】

さらに、記録媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張カードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張カードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【０１１２】

本発明を上記記録媒体に適用する場合、その記録媒体には、先に説明したフローチャートに対応するプログラムコードが格納されることになる。

【０１１３】

本発明の実施態様の例を以下に列挙する。

（実施態様１）　所定の作者により作成された原データを処理する情報処理装置であって、上記原データを変更する際に、その変更に関する変更情報を記憶媒体に記憶する変更情報記憶手段と、上記変更情報が原本であることを保証するための変更保証情報を作成する変更保証情報作成手段とを有することを特徴とする

情報処理装置。

【０１１４】

（実施態様２）　上記原データが原本であることを保証するための原データ保証情報を作成する原データ保証情報作成手段をさらに有することを特徴とする実施態様１に記載の情報処理装置。

【０１１５】

（実施態様３）　上記原データを変更することが指示された際に、上記指示された内容に従って上記原データを変更する処理を行うための変更処理手段をさらに有することを特徴とする実施態様１または２に記載の情報処理装置。

【０１１６】

（実施態様４）　上記変更保証情報と、上記原データ保証情報は、デジタル署名であることを特徴とする実施態様１～３の何れか１項に記載の情報処理装置。

【０１１７】

（実施態様５）　上記変更情報は、上記原データを特定する情報と、上記変更処理手段を特定する情報と、上記原データを変更する際に行った変換処理を特定する情報とを含むことを特徴とする実施態様１～４の何れか１項に記載の情報処理装置。

【０１１８】

（実施態様６）　上記変更情報は、上記原データと、上記原データに対する変更データとの差分情報を含むことを特徴とする実施態様１～５の何れか１項に記載の情報処理装置。

【０１１９】

（実施態様７）　上記原データと、上記原データ保証情報と、上記変更情報と、上記変更保証情報とを一体として管理する管理手段をさらに有することを特徴とする実施態様１～６の何れか１項に記載の情報処理装置。

【０１２０】

（実施態様８）　上記原データと、上記原データ保証情報と、上記変更情報と、上記変更保証情報とを一体として送付する送付手段をさらに有することを特徴とする実施態様１～７の何れか１項に記載の情報処理装置。

【０１２１】

（実施態様９）　所定の作者により作成された原データを処理する情報処理装置であって、上記原データが正当なものであることを確認する原データ確認手段と、上記原データの変更に関する変更情報が正当なものであることを確認する変更情報確認手段と、上記原データと上記変更情報が正当であることが確認された場合に、上記変更情報に応じて上記原データを変更する原データ変更手段とを有することを特徴とする情報処理装置。

【０１２２】

（実施態様１０）　上記原データ確認手段は、上記原データに対するデジタル署名を検証し、上記変更情報確認手段は、上記変更情報に対するデジタル署名を検証するようにしたことを特徴とする実施態様９に記載の情報処理装置。

【０１２３】

（実施態様１１）　所定の作者により作成された原データを処理する情報処理装置であって、上記原データの変更に関する変更情報と、上記原データの変更履歴とを管理する管理手段を有することを特徴とする情報処理装置。

【０１２４】

（実施態様１２）　ネットワークに接続された上記実施態様１～１１の何れか１項に記載の情報処理装置を複数有し、上記複数の情報処理装置は、上記ネットワーク上で共有された電子データが正当なものであることと、上記電子データの変更に関する第１の変更情報が正当なものであることとを確認する確認手段と、上記電子データと、上記第１の変更情報とが、上記確認手段により正当なものであることが確認された場合に、上記電子データを変更する電子データ変更手段と、上記電子データ変更手段により変更された電子データの変更に関する第２の変更情報と、上記第２の変更情報が正当なものであることを保証するための変更保証情報とを作成する情報作成手段と、上記情報作成手段により作成された第２の変更情報と、変更保証情報とを上記ネットワークに送信する送信手段とを有し、上記複数の情報処理装置で共同して上記電子データの作成と管理を行うようにしたことを特徴とする電子データ管理システム。

【０１２５】

（実施態様１３）　上記第１及び第２の変更情報と、上記原データの変更履歴を表す情報とのうち、少なくとも何れか一方を管理する変更履歴管理手段を有し、上記変更履歴管理手段を利用して上記複数の情報処理装置で共同して上記電子データを作成することを特徴とする実施態様１２に記載の電子データ管理システム。

【０１２６】

（実施態様１４）　上記複数の情報処理装置は、上記電子データ及び上記第１の変更情報のうち少なくとも何れか一方が正当でないということが上記確認手段により確認された場合に、その旨を他の情報処理装置に通知する通知手段をさらに有することを特徴とする実施態様１２または１３に記載の電子データ管理システム。

【０１２７】

（実施態様１５）　１次著作物の著作者が所有する第１の情報処理装置と、上記第１の情報処理装置とネットワークを介して接続された第２～第ｎの情報処理装置とを有し、上記第２～第ｎの情報処理装置のうち、上記著作者が正当と認めたユーザが所有する情報処理装置に対して、上記第１の情報処理装置から上記１次著作物を配布する１次著作物配布手段と、上記１次著作物配布手段により１次著作物が配布された情報処理装置により、上記著作者から認められた許諾範囲内で１次著作物を変更し、その変更内容を表す変更情報と、その変更情報が原本であることを保証するための第１の変更保証情報情報とを、上記第１の情報処理装置に送信する送信手段と、上記変更情報と上記第１の変更保証情報との送信先である上記第１の情報処理装置により、上記送信された変更情報が正当なものであることを、上記第１の変更保証情報を用いて確認し、正当であることを確認した場合に、上記送信された変更情報が正当なものであることを保証するための第２の変更保証情報を上記変更情報に付加して送信元の情報処理装置に返信する返信手段とを有し、上記変更情報と、上記第２の変更保証情報とが返信された情報処理装置に対して、上記１次著作物を変更したものを２次著作物として使用することを許諾するようにしたことを特徴とする著作物管理システム。

【０１２８】

（実施態様１６）　所定の作者により作成された原データを処理する情報処理方法であって、上記原データを変更する際に、その変更に関する変更情報を記憶媒体に記憶する変更情報記憶処理と、上記変更情報が原本であることを保証するための変更保証情報を作成する変更保証情報作成処理とを行うことを特徴とする情報処理方法。

【０１２９】

（実施態様１７）　上記原データが原本であることを保証するための原データ保証情報を作成する原データ保証情報作成処理をさらに行うことを特徴とする実施態様１６に記載の情報処理方法。

【０１３０】

（実施態様１８）　上記原データと、上記原データ保証情報と、上記変更情報と、上記変更保証情報とを一体として管理する管理処理をさらに行うことを特徴とする実施態様１６または１７に記載の情報処理方法。

【０１３１】

（実施態様１９）　上記原データと、上記原データ保証情報と、上記変更情報と、上記変更保証情報とを一体として送付する送付処理をさらに行うことを特徴とする実施態様１６～１８の何れか１項に記載の情報処理方法。

【０１３２】

（実施態様２０）　所定の作者により作成された原データを処理する情報処理方法であって、上記原データが正当なものであることを確認する原データ確認処理と、上記原データの変更に関する変更情報が正当なものであることを確認する変更情報確認処理と、上記原データと上記変更情報が正当であることが確認された場合に、上記変更情報に応じて上記原データを変更する原データ変更処理とを行うことを特徴とする情報処理方法。

【０１３３】

（実施態様２１）　上記原データ確認処理は、上記原データに対するデジタル署名を検証し、上記変更情報確認処理は、上記変更情報に対するデジタル署名を検証するようにしたことを特徴とする実施態様２０に記載の情報処理方法。

【０１３４】

（実施態様２２）　所定の作者により作成された原データを処理する情報処理方法であって、上記原データの変更に関する変更情報と、上記原データの変更履歴とを管理する管理処理を行うことを特徴とする情報処理方法。

【０１３５】

（実施態様２３）　ネットワーク上で共有された電子データが正当なものであることと、上記電子データの変更に関する第１の変更情報が正当なものであることとを確認する確認処理と、上記電子データと、上記第１の変更情報とが、上記確認処理により正当なものであることが確認された場合に、上記電子データを変更する電子データ変更処理と、上記電子データ変更処理により変更された電子データの変更に関する第２の変更情報と、上記第２の変更情報が正当なものであることを保証するための変更保証情報とを作成する情報作成処理と、上記情報作成処理により作成された第２の変更情報と、変更保証情報とを上記ネットワークに送信する送信処理とを行うことを特徴とする情報処理方法。

【０１３６】

（実施態様２４）　上記第１及び第２の変更情報と、上記原データの変更履歴を表す情報とのうち、少なくとも何れか一方を管理する変更履歴管理処理をさらに行うことを特徴とする実施態様２３に記載の情報処理方法。

【０１３７】

（実施態様２５）　上記電子データ及び上記第１の変更情報のうち少なくとも何れか一方が正当でないということが上記確認処理により確認された場合に、その旨を通知する通知処理をさらに行うことを特徴とする実施態様２３または２４に記載の情報処理方法。

【０１３８】

（実施態様２６）　著作者が正当と認めたユーザが所有する情報処理装置に対して、上記著作者が所有する第１の情報処理装置から１次著作物を配布する１次著作物配布処理と、上記１次著作物配布処理により１次著作物が配布された情報処理装置により、上記著作者から認められた許諾範囲内で１次著作物を変更し、その変更内容を表す変更情報と、その変更情報が原本であることを保証するための第１の変更保証情報情報とを、上記第１の情報処理装置に送信する送信処理と

、上記変更情報と上記第１の変更保証情報との送信先である上記第１の情報処理装置により、上記送信された変更情報が正当なものであることを、上記第１の変更保証情報を用いて確認し、正当であることを確認した場合に、上記送信された変更情報が正当なものであることを保証するための第２の変更保証情報を上記変更情報に付加して送信元の情報処理装置に返信する返信処理とを行い、上記変更情報と、上記第２の変更保証情報とが返信された情報処理装置に対して、上記１次著作物を変更したものを２次著作物として使用することを許諾するようにしたことを特徴とする情報処理方法。

【０１３９】

（実施態様２７）　所定の作者により作成された原データを変更する際に、その変更に関する変更情報を記憶媒体に記憶する変更情報記憶処理と、上記変更情報が原本であることを保証するための変更保証情報を作成する変更保証情報作成処理とをコンピュータに実行させることを特徴とするコンピュータプログラム。

【０１４０】

（実施態様２８）　所定の作者により作成された原データが正当なものであることを確認する原データ確認処理と、上記原データの変更に関する変更情報が正当なものであることを確認する変更情報確認処理と、上記原データと上記変更情報が正当であることが確認された場合に、上記変更情報に応じて上記原データを変更する原データ変更処理とをコンピュータに実行させることを特徴とするコンピュータプログラム。

【０１４１】

（実施態様２９）　所定の作者により作成された原データの変更に関する変更情報と、上記原データの変更履歴とを管理する管理処理をコンピュータに実行させることを特徴とするコンピュータプログラム。

【０１４２】

（実施態様３０）　ネットワーク上で共有された電子データが正当なものであることと、上記電子データの変更に関する第１の変更情報が正当なものであることとを確認する確認処理と、上記電子データと、上記第１の変更情報とが、上記確認処理により正当なものであることが確認された場合に、上記電子データを変

更する電子データ変更処理と、上記電子データ変更処理により変更された電子データの変更に関する第２の変更情報と、上記第２の変更情報が正当なものであることを保証するための変更保証情報とを作成する情報作成処理と、上記情報作成処理により作成された第２の変更情報と、変更保証情報とを上記ネットワークに送信する送信処理とをコンピュータに実行させることを特徴とするコンピュータプログラム。

【０１４３】

（実施態様３１）　著作者が正当と認めたユーザが所有する情報処理装置に対して、上記著作者が所有する第１の情報処理装置から１次著作物を配布する１次著作物配布処理と、上記１次著作物配布処理により１次著作物が配布された情報処理装置により、上記著作者から認められた許諾範囲内で１次著作物を変更し、その変更内容を表す変更情報と、その変更情報が原本であることを保証するための第１の変更保証情報情報とを、上記第１の情報処理装置に送信する送信処理と、上記変更情報と上記第１の変更保証情報との送信先である上記第１の情報処理装置により、上記送信された変更情報が正当なものであることを、上記第１の変更保証情報を用いて確認し、正当であることを確認した場合に、上記送信された変更情報が正当なものであることを保証するための第２の変更保証情報を上記変更情報に付加して送信元の情報処理装置に返信する返信処理とを行い、上記変更情報と、上記第２の変更保証情報とが返信された情報処理装置に対して、上記１次著作物を変更したものを２次著作物として使用することを許諾するようにしたことをコンピュータに実行させることを特徴とするコンピュータプログラム。

【０１４４】

（実施態様３２）　上記実施態様２７～３１の何れか１項に記載のコンピュータプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【０１４５】

【発明の効果】

以上説明したように本発明によれば、所定の作者により作成された原データを変更する際に、その変更に関する変更情報を記憶媒体に記憶するとともに、上記

変更情報が原本であることを保証するための変更保証情報を作成するようにしたので、上記変更保証情報に基づいて上記原データの変更が正当なものであるか否かを判断し、正当なものである場合には上記変更情報により上記原データを変更することができるようになる。したがって、上記原データの原本性を保証しながら、上記原データの作者が認める正当な変更を行うことができ、上記原データの原本性と、データの最新性の両方を保証することができる。また、上記変更情報により、上記原データと、変更したデータとの関係を知ることができ、上記原データと、変更したデータとが適切な関係にあることを保証することができる。さらに、上記変更情報は、上記変更したデータそのものに比べてデータ量が少ないので、上記原データを変更するのに要する記憶容量を可及的に小さくすることができる。

【図面の簡単な説明】

【図１】

本発明の第１の実施の形態を示し、記録媒体に記録される原画像、署名、及び履歴情報を示した概念図である。

【図２】

本発明の第１の実施の形態を示し、電子署名を生成する際の処理を説明するフローチャートである。

【図３】

本発明の第１の実施の形態を示し、電子署名を検証する際の処理を説明するフローチャートである。

【図４】

本発明の第１の実施の形態を示し、情報処理装置の構成の一例を示したブロック図である。

【図５】

本発明の第２の実施の形態を示し、記録媒体に記録される原画像、署名、及び履歴情報を示した概念図である。

【図６】

本発明の第２の実施の形態を示し、履歴情報と電子署名とを処理ごとにまとめ

たリストの一例を示した図である。

【図７】

本発明の第３の実施の形態を示し、電子データ管理システムの構成の一例を示したブロック図である。

【図８】

本発明の第５の実施の形態を示し、著作物管理システムで行われる処理を説明するフローチャートである。

【符号の説明】

１１、１４、１６　電子署名

１２　原画像

１３、１５　履歴情報

３０１　情報処理装置

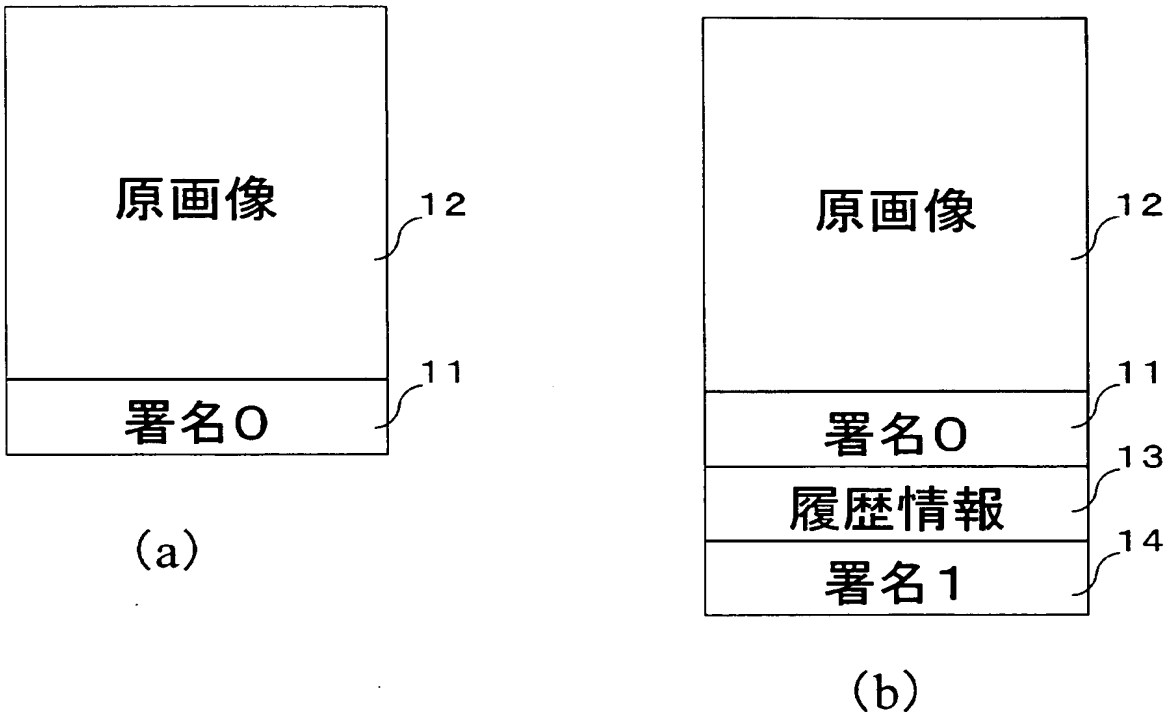
６０１　サーバ

６０２　電子文書

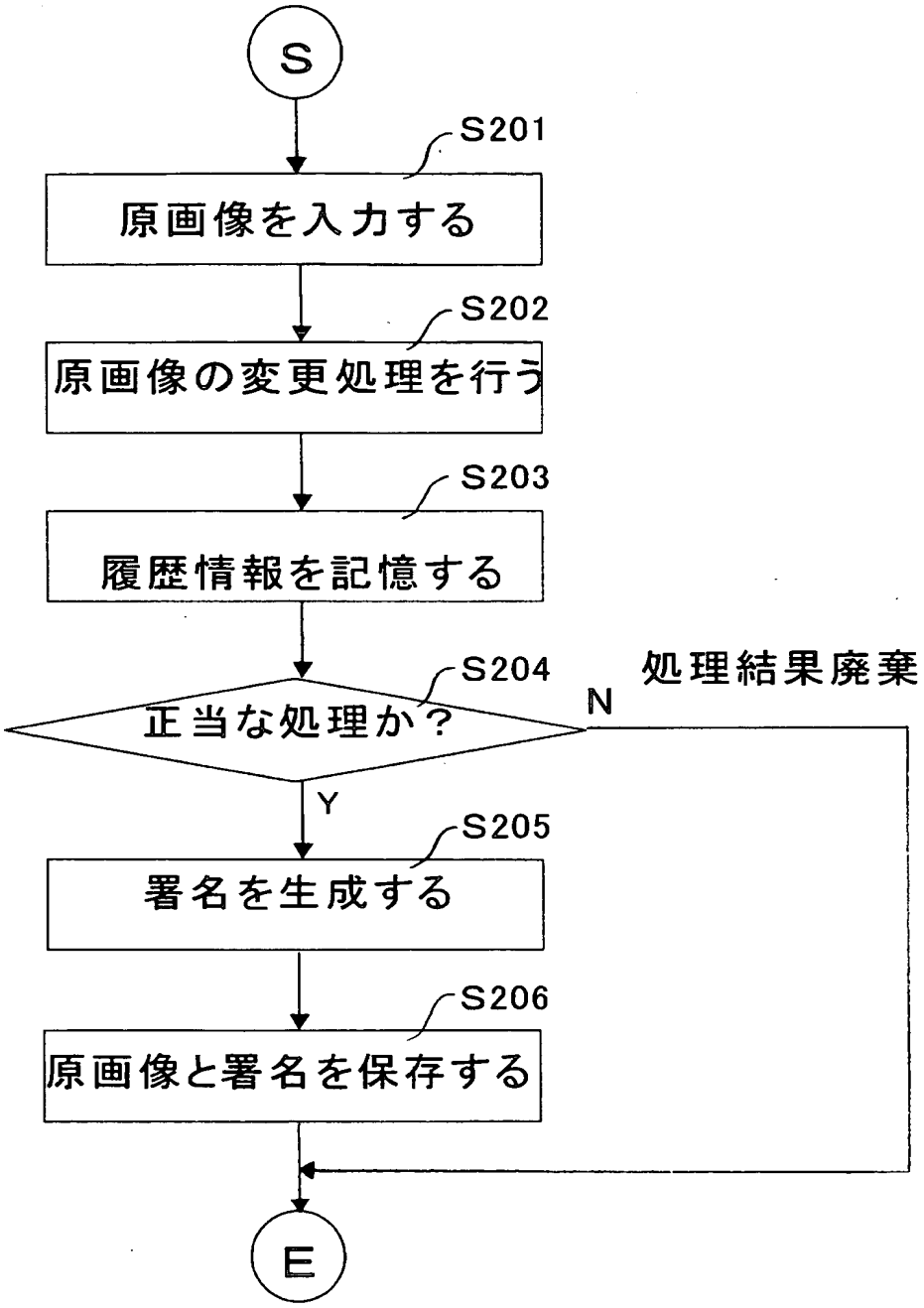
６０３～６０５　ユーザ

【書類名】　図面

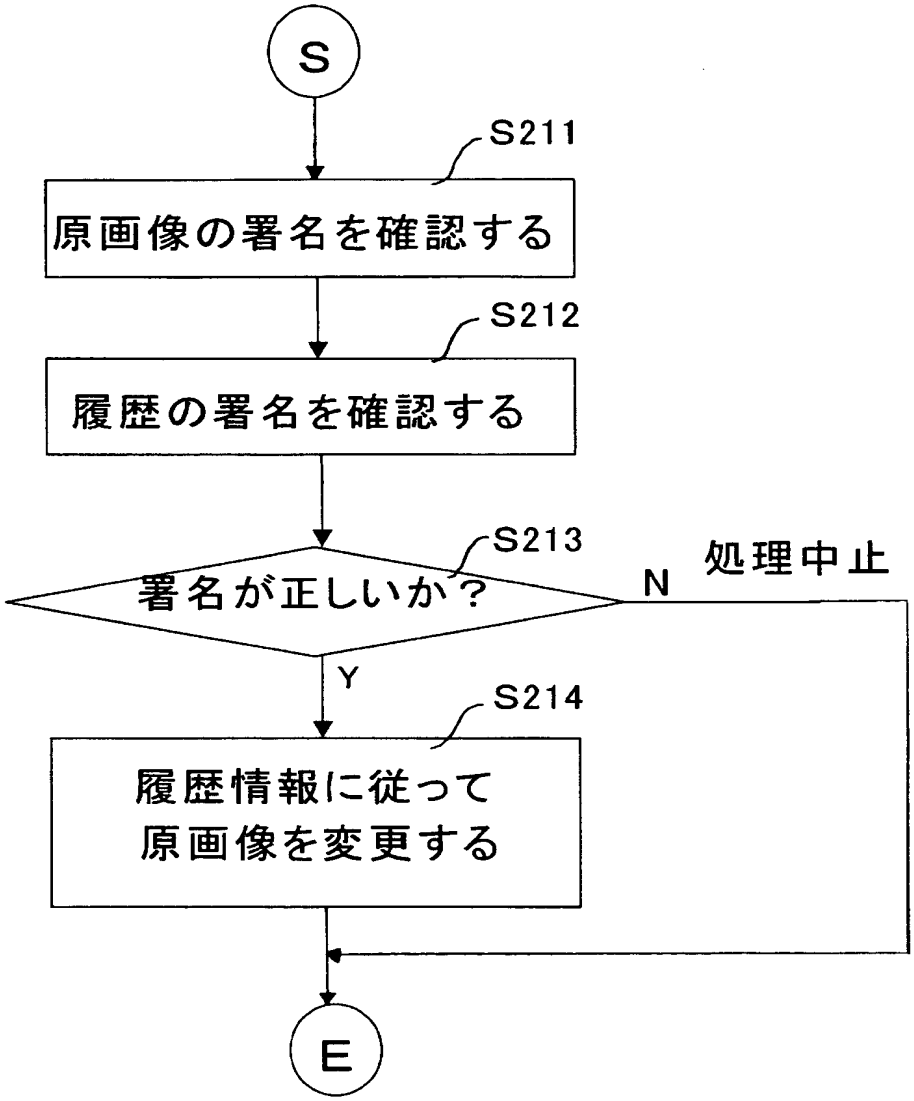
【図１】



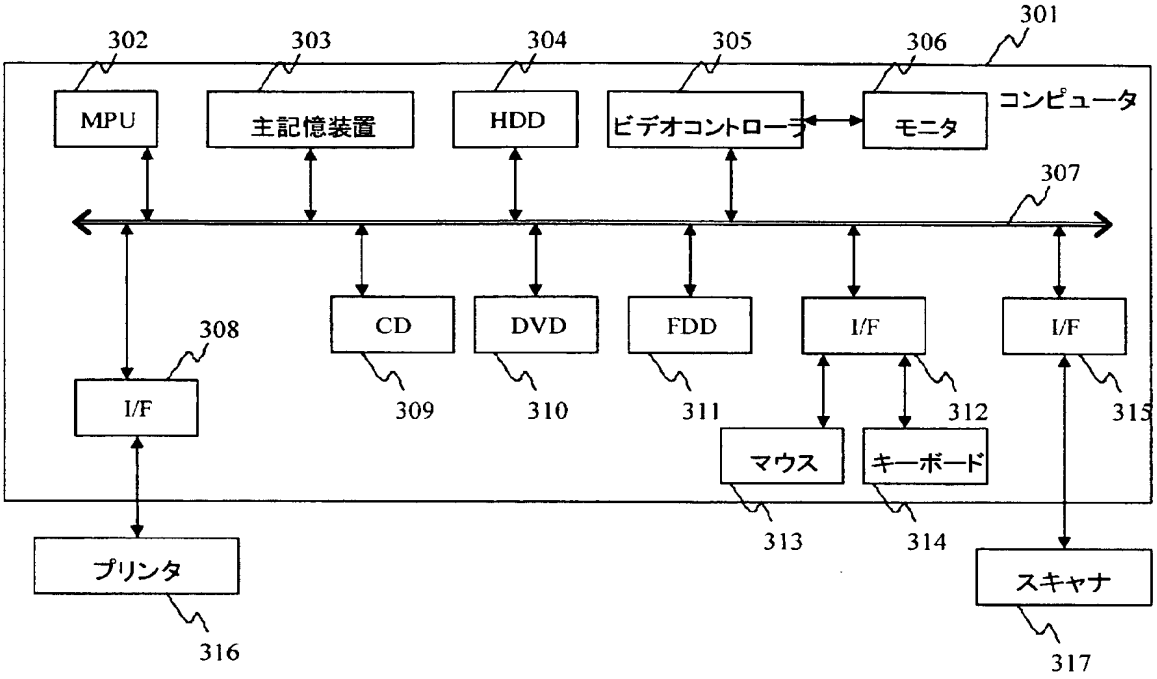
【図２】


S
S201
原画像を入力する
S202
原画像の変更処理を行う
S203
履歴情報を記憶する
S204
正当な処理か？
N
処理結果廃棄
Y
S205
署名を生成する
S206
原画像と署名を保存する
E

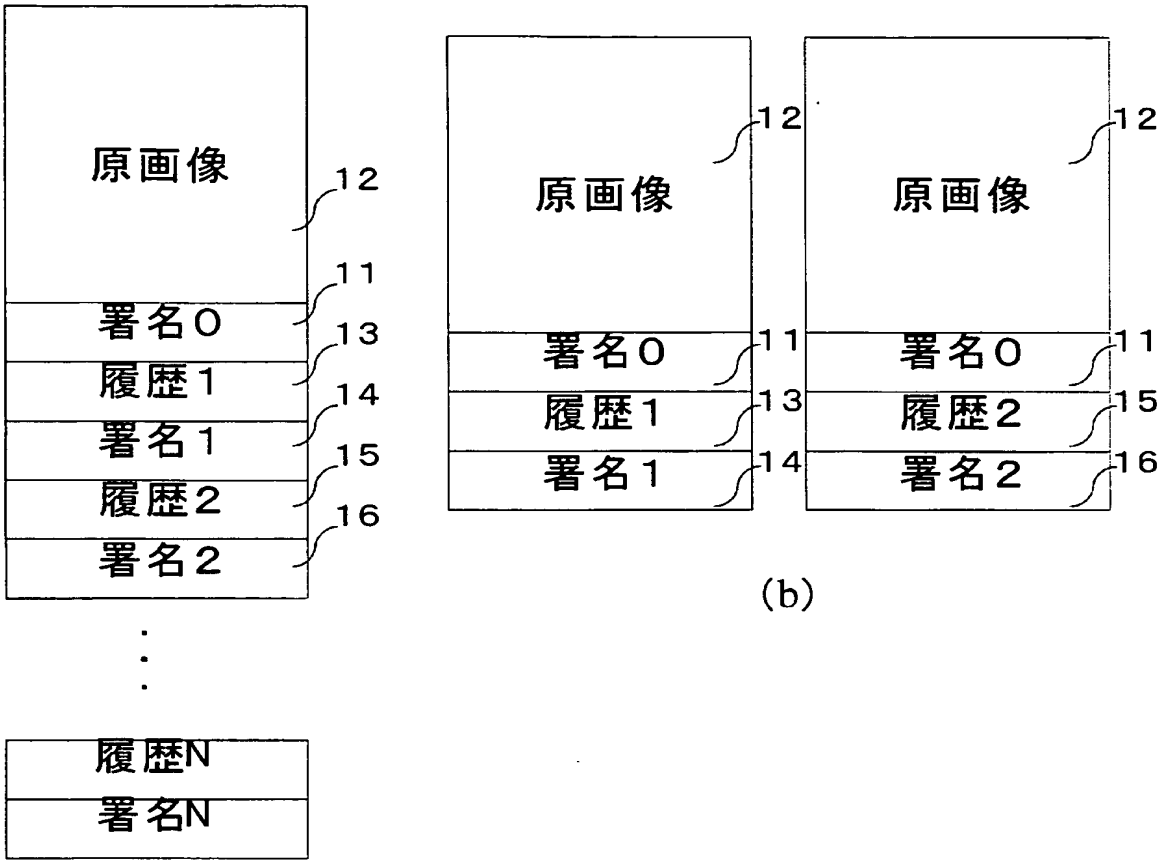
【図３】


S
S211
原画像の署名を確認する
S212
履歴の署名を確認する
S213
署名が正しいか？
N
処理中止
Y
S214
履歴情報に従って
原画像を変更する
E

【図４】


301
302
303
304
305
306
コンピュータ
MPU
主記憶装置
HDD
ビデオコントローラ
モニタ
307
308
CD
DVD
FDD
I/F
I/F
I/F
309
310
311
312
315
マウス
キーボード
313
314
プリンタ
スキャナ
316
317

【図５】

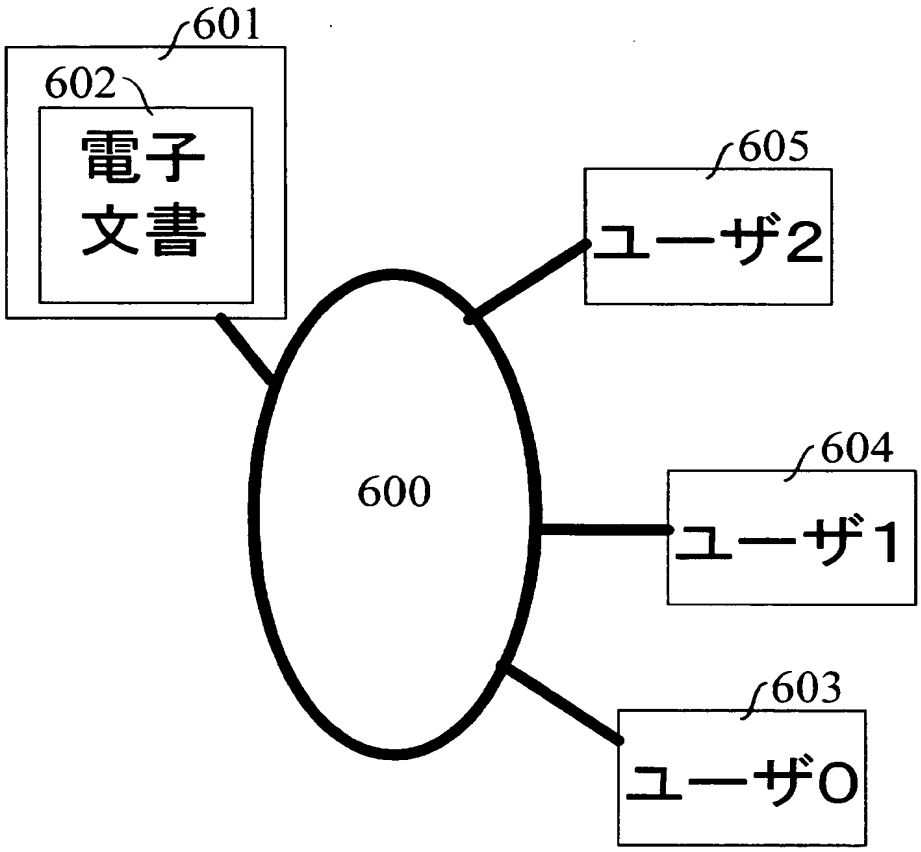

原画像
12
署名０
11
履歴１
13
署名１
14
履歴２
15
署名２
16
履歴N
署名N
(a)
原画像
12
署名０
11
履歴１
13
署名１
14
原画像
12
署名０
11
履歴２
15
署名２
16
(b)

【図６】

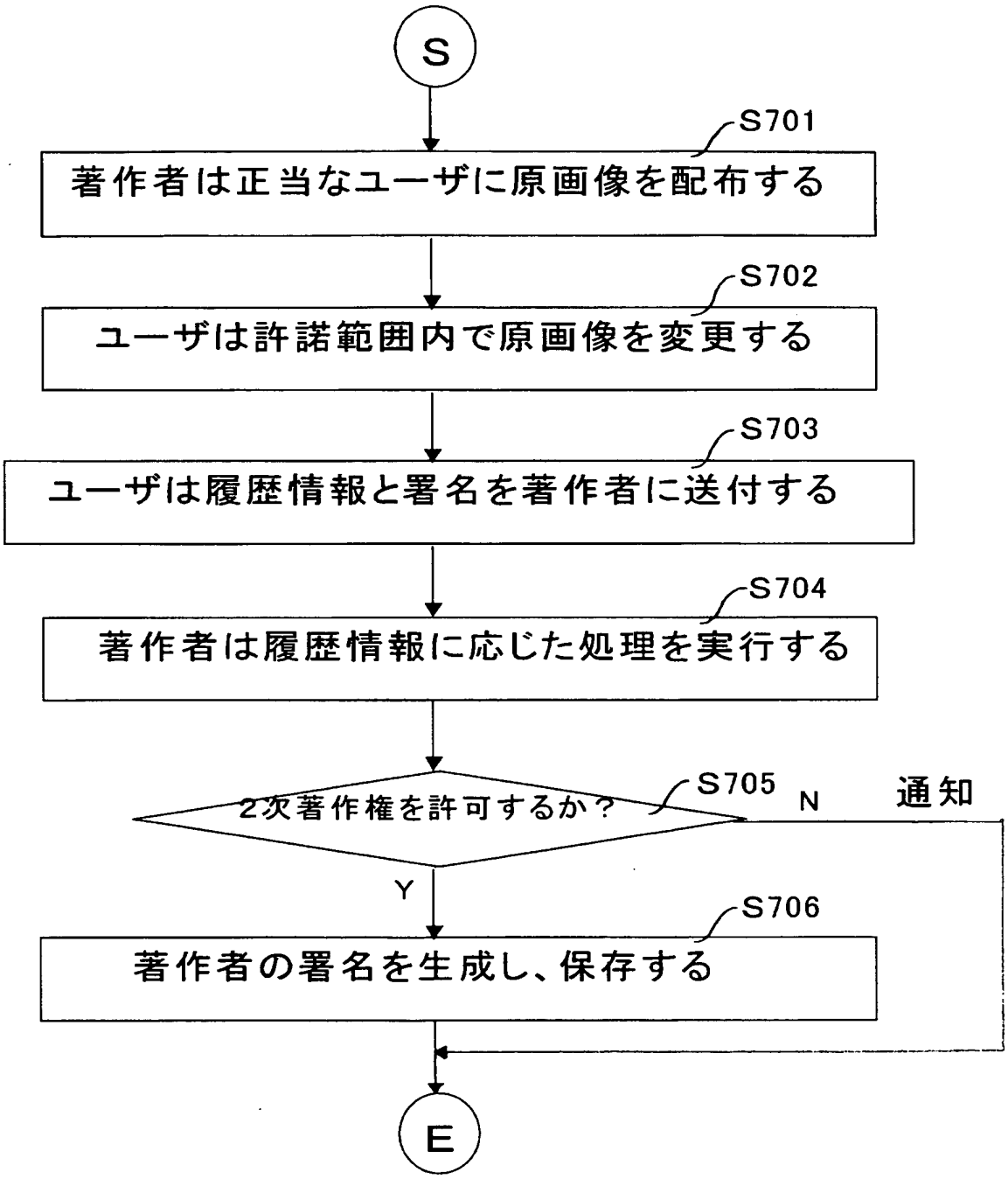
60

履歴情報	電子署名	用途
履歴1	署名1	輝度変換
履歴2	署名2	切り取り
・ ・ ・	・ ・ ・	・ ・ ・

【図７】



【図８】


S
S701
著作者は正当なユーザに原画像を配布する
S702
ユーザは許諾範囲内で原画像を変更する
S703
ユーザは履歴情報と署名を著作者に送付する
S704
著作者は履歴情報に応じた処理を実行する
S705
2次著作権を許可するか？
N
通知
Y
S706
著作者の署名を生成し、保存する
E

【書類名】　　要約書

【要約】

【課題】　データの原本性を保証しながら、上記データの作者が認める正当な変更を行えるようにする。

【解決手段】　所定の作者により作成された原画像１２を変更する際に、その変更に関する履歴情報１３と、履歴情報１３が原本であることを保証するための第２の署名（署名１）１４とを作成することにより、上記作者や第三者が、上記変更が正当なものであるか否かを上記変更保証情報により判断することが可能になるようにする。これにより、原画像１２の原本性を保証しながら、原画像１２の作者が認める正当な変更を行えるようになる。

【選択図】　　図１

特願２００２－３３２５７７

出　願　人　履　歴　情　報

識別番号　　［０００００１００７］

１．変更年月日　　１９９０年　８月３０日
［変更理由］　　新規登録
住　所　　東京都大田区下丸子３丁目３０番２号
氏　名　　キヤノン株式会社